REMARKS

Applicant and his attorney wish to thank Supervisory Primary Examiner Pham for the courtesy of the telephone interview held November 8, 2005. The substantive matters discussed at that interview are set forth in the Written Statement Of Reasons Warranting Favorable Action Presented At Interview filed on the same day as this Response.

This paper is responsive to the Office action mailed on May 24, 2005. Favorable reconsideration is requested.

Claims 1-61 are now in the application.

Claims 28-61 have been added to the application and claim various aspects of the invention neither shown or suggested by the references of record. Applicant submits that all claims, including new claims 28-61, are allowable.

First Rejection of Office Action

Claims 1-27 have been rejected for anticipation by U.S. Patent Application No. 2003/0005331 ("Williams"). That rejection is respectfully traversed for the failure of Williams to include all elements and limitations of the rejected claims.

Axiomatically, rejection of a claim for anticipation by a reference requires that the reference contain, explicitly or inherently, all of the steps (or elements) and limitations of the rejected claim.

Independent Claim 1:

In independent claim 1, as a representative claim, a combination is set forth for providing a security network system. Claim 1 requires "a plurality of said one or more networked systems comprising a hardware processor providing transport layer protocol processing" and also "said security system providing multiple protocol layer security in said network." Nowhere in Williams is a plurality of networked systems comprising a hardware processor providing transport layer protocol processing and multiple protocol layer security described or suggested.

The Examiner has stated that Williams teaches a security network system that operates by providing security at two or more network layers of the OSI model as shown in Figure 4 and descriptions in paragraphs 0073 and 0076. Applicant respectfully disagrees. First, Williams clearly articulates in the Summary of the Invention [0025, page 2] that the invention is for security at OSI layer 3 as: "It is a further object of the invention to provide a secure network in which the security mechanisms are ***at*** layer 3 of protocol hierarchy". Second, the paragraph cited by the Examiner [0073] also clearly articulates that the security devices operate *at* layer 3 of protocol hierarchy as stated in line 3 of 0073 as: "The devices 18 operate ***within*** layer 3 of the protocol hierarchy and provide a cryptographic foundation that assures communications secrecy and communicates integrity". Further, paragraph 0076 states: "The distinction between Region C and Region D is that hosts in Region C are trusted MLS computers that are capable of simultaneously processing data at multiple security levels, while hosts in Region D are not capable of simultaneously processing data at multiple security levels." It is not clear from the Office action exactly what from this paragraph the Examiner considers Region C providing layer-4 security protection. However, it appears that the Examiner may consider it to be the MLS (Multi-Level Security) or multiple levels of security. If so, Multiple Level Security is defined by Williams in paragraph 0003 (page 1) and described again in paragraph 110 (page 7) and Figure 6 as follows: "The term `multi-level security` refers to a system in which two or more classification levels of information are processed simultaneously, and not all users are cleared for all levels of information present" (see [0003]) and "As shown in FIG. 6, the network 10 is capable of supporting up to 256 hierarchical security levels and at least 65,535 non-hierarchical categories" (see [0110]). Thus it is very clear from Williams that multiple level security has 256 security levels which are totally different from an OSI model with seven layers which is referred to in claim 1 of Applicant's invention stated as: "said security system providing multiple protocol layer security in the said network".

Accordingly, Williams does not explicitly teach, disclose, or illustrate each and every element of claim 1. Further, if each element of claim 1 is considered by the Examiner to be inherent in Williams, Applicant respectfully requests the introduction of extrinsic evidence clearly showing that the omitted material is necessarily present in Williams and that it would be so recognized by persons of ordinary skill. In this regard, see In re Robertson, 49 USPQ2d 1949 (Fed. Cir. 1999). Alternatively, Applicant respectfully requests withdrawal of this rejection.

Claims 3-8, 17 and 19, depending from allowable claim 1, are also allowable for the same reasons stated above.

Independent Claim 2:

Regarding independent claim 2, a combination is set forth for providing a security system for a storage area network. Williams does not teach, describe or suggest any elements of providing a security system for a storage area network.

In addition, the Examiner acknowledges at page 4, third paragraph, of the Office action that "Williams is silent regarding a storage area network (SAN)" as required by claim 2.

Accordingly, Williams does not explicitly teach, disclose, or illustrate each and every element of claim 2. Further, if each element of claim 2 is considered by the Examiner to be inherent in Williams, Applicant respectfully requests the introduction of extrinsic evidence clearly showing that the omitted material is necessarily present in Williams and that it would be so recognized by persons of ordinary skill. In this regard, see In re Robertson, 49 USPQ2d 1949 (Fed. Cir. 1999). Alternatively, Applicant respectfully requests withdrawal of this rejection.

Claims 20-25, depending from allowable claim 2, are also allowable.

Independent Claim 9:

Regarding claim 9, a combination is set forth for providing a security network system. The first element requires "a plurality of said one or more networked systems comprising a hardware processor providing remote direct memory access capability." Nowhere in Williams is plurality of networked systems comprising a hardware processor providing remote direct memory access capability described or suggested. On the contrary, Williams clearly states that there is no interface by which another host (i.e. remote host) can retrieve data from the security devices' memory buffers in paragraph 0175 page 11 as stated by: "Further, except for control requests from NSC 12, which are accepted only from NSC and must be cryptographically verified, there is no interface by which another host on the network can retrieve data from the security device's internal buffers". Further, in paragraph 0184, page 12, Williams clearly articulates that direct access to the memory cannot be established as stated in the second line

of paragraph 0184 as: "Thus, direct access cannot be established to the local RAM 54, network coprocessor 66, encryption hardware 58, or authentication interface 60".

The Examiner also stated that Williams teaches a security network system that operates by providing security at two or more network layers of the OSI model as shown in Figure 4 and descriptions in paragraphs 0073 and 0076. Applicant respectfully disagrees for the same reasons as discussed above for claim 1.

Accordingly, Williams does not explicitly teach, disclose, or illustrate each and every element of claim 9. Further, if each element of claim 9 is considered by the Examiner to be inherent in Williams, Applicant respectfully requests the introduction of extrinsic evidence clearly showing that the omitted material is necessarily present in Williams and that it would be so recognized by persons of ordinary skill. In this regard, see In re Robertson, 49 USPQ2d 1949 (Fed. Cir. 1999). Alternatively, Applicant respectfully requests withdrawal of this rejection.

Claims 10-16, and 18, depending from allowable claim 9, are also allowable.

Independent Claim 26:

Regarding claim 26, a combination is set forth for providing a security network system. The first element requires "a plurality of said set of systems comprising a hardware processor providing transport layer protocol processing" and also "said security system providing multiple protocol layer security in said network." Nowhere in Williams is a plurality of networked systems comprising a hardware processor providing transport layer protocol processing and multiple protocol layer security described or suggested.

The Examiner also stated that Williams teaches a security network system that operates by providing security at two or more network layers of the OSI model as shown in Figure 4 and descriptions in paragraphs 0073 and 0076. Applicant respectfully disagrees for the same reasons as discussed above for claim 1.

Accordingly, Williams does not explicitly teach, disclose, or illustrate each and every element of claim 26. Further, if each element of claim 26 is considered by the Examiner to be inherent in Williams, Applicant respectfully requests the introduction of extrinsic evidence clearly showing that the omitted material is necessarily present in Williams and that it would be so

recognized by persons of ordinary skill. In this regard, see In re Robertson, 49 USPQ2d 1949 (Fed. Cir. 1999). Alternatively, Applicant respectfully requests withdrawal of this rejection.

Independent Claim 27:

Regarding claim 27, a combination is set forth for providing a security network system. The first element requires "at least one of said networked systems having a hardware processor providing a protocol processing stack". Nowhere in Williams is a hardware processor providing a protocol processing stack described or suggested.

The Examiner has stated that Williams teaches a unique policy driver in [0032] to set up the hardware to handle the enforcement of policy rules. It is not clear from the Office action exactly what from this paragraph the Examiner considers a unique policy driver. There is reference to a unique policy in [0032] as stated in: "Cryptography provides the underlying secrecy and integrity of communications required for the network to be able to enforce a unique policy when operating over an open backbone network". There is nothing referred to as a "policy driver" in this paragraph as asserted by the Examiner. Further, as discussed above, since there is no hardware processor providing a protocol processing stack described or suggested by Williams, there obviously is no policy driver for the same taught by Williams.

Applicant's claim 27 further requires "a central manager for compiling and distributing said rules and monitoring the enforcement of said rules and said hardware processor". Examiner states that the policy is in the form of a software driver and handled by a central manager device (DAC) as described in [0129] of Williams. It is not clear from the Office action exactly what from this paragraph the Examiner considers a central manager "compiling and distributing" the rules. However, if the Examiner considers the network security administrator specifying the policy rules at the NSC and downloading it to each security device in Williams as that, it is not clear that the operations constitute "compiling and distributing" the rules to security devices as required by Applicant's invention.

Accordingly, Williams does not explicitly teach, disclose, or illustrate each and every element of claim 27. Further, if each element of claim 27 is considered by the Examiner to be inherent in Williams, Applicant respectfully requests the introduction of extrinsic evidence clearly showing that the omitted material is necessarily present in Williams and that it would be so

recognized by persons of ordinary skill. In this regard, see In re Robertson, 49 USPQ2d 1949 (Fed. Cir. 1999). Alternatively, Applicant respectfully requests withdrawal of this rejection.

Second Rejection of Office Action

Claims 2 and 20-25 were rejected under 35 USC §103(a) as being unpatentable over Williams in view of Twomey (U.S. Patent Application No. 2003/0131228).

As to claims 2 and 20-25, the Examiner stated that:

"Williams teaches all of the above described features, however, Williams is silent regarding a storage area network (SAN). Twomey discloses a system for a SAN that handles both secure and regular types of network security (see [0006, 0027]).

Motivation to combine the SAN of Twomey with security network of Williams is evident from background portions of their respective specifications. For instance, Williams discloses the need for security networks that operate at various layers of the network layer hierarchy and provide centralized administration (emphasis added).... Similarly, Twomey discloses the need to provide encryption for a network system to prevent unauthorized access to a private network (see [0034]). The system includes a security processor for handling secure data traffic and utilizes security protocols (i.e. Ipsec)."

Independent Claim 2:

As a first reason that the obviousness rejection is incorrect, Applicant respectfully asserts that Williams does not teach all of the described features of claim 2. Further, a combination of Williams and Twomey also does not teach all of the described features of claim 2.

That is, a combination is set forth for providing a security system for storage area network in claim 2. The claim requires "a plurality of said set of [one or more networked] systems comprising a hardware processor providing transport layer protocol processing." Nowhere in Williams is plurality of networked systems comprising a hardware processor providing transport layer protocol processing described or suggested. As stated by the Examiner, Williams is silent regarding a SAN but Twomey discloses a system for a SAN.

Twomey does talk about protocol processing in a few places in the application (e.g. in paragraph 0042 protocol processing is defined as "On the other hand, if the packet is not encrypted, the first integrated processor 22A may perform protocol processing on the packet)... . The protocol processing may include, for example, determining the target of the packet on the switch fabric (e.g. a storage device in the embodiment of Fig 1) and transmitting information to the switch fabric card indicating the target for routing of the packet to the target. The memory 26A may include various databases which may be used in protocol processing (e.g. database mapping IP addresses to switch fabric addresses or other routing information)". Thus Twomey defines IP address look-up and transmitting the information as protocol processing. Prior to this, paragraph 0039 states packet processing as "a set of flowcharts are shown illustrating various operations of one embodiment of the integrated processors 22A-22B for processing packets. More particularly, the flowcharts of FIGs. 3-7 may represent the operation of integrated processors 22A-22B when executing sets of instructions programmed for the integrated processors." Neither this description nor the flow charts in Twomey describe or suggest a transport layer protocol processing. Thus, nowhere in Williams or Twomey is plurality of networked systems comprising a hardware processor providing transport layer protocol processing (and providing multiple protocol layer security) described or suggested.

As a second reason that the obviousness rejection is incorrect, Applicant respectfully asserts that Williams does not teach a security network system that operates by providing security at various network layers of the network layer hierarchy unlike the assertion by the Examiner. Further, a combination of Williams and Twomey also does not teach the same. First, Williams clearly articulates in the Summary of the Invention [0025, page 2] that the invention is for security at OSI layer 3 as: "It is a further object of the invention to provide a secure network in which the security mechanisms are at layer 3 of protocol hierarchy". Second, the paragraph cited by the Examiner [0073] also clearly articulates that the security devices operate at layer 3 of protocol hierarchy as stated in line 3 of 0073 as: "The devices 18 operate within layer 3 of the protocol hierarchy and provide a cryptographic foundation that assures communications secrecy and communicates integrity". Further, paragraph 0076 states: "The distinction between Region C and Region D is that hosts in Region C are trusted MLS computers that are capable of simultaneously processing data at multiple security levels, while hosts in Region D are not capable of simultaneously processing data at multiple security levels." Multiple Level Security is defined by Williams in paragraph 0003 (page 1) and described again

in paragraph 110 (page 7) and Figure 6 as follows: "The term `multi-level security` refers to a system in which two or more classification levels of information are processed simultaneously, and not all users are cleared for all levels of information present" (see [0003]) and "As shown in FIG. 6, the network 10 is capable of supporting up to 256 hierarchical security levels and at least 65,535 non-hierarchical categories" (see [0110]). Thus it is very clear from Williams that multiple level security has 256 security levels which is totally different from OSI model with seven protocol layers which is referred in claim 2 in Applicant's invention stated as: "said security system providing multiple protocol layer security in the said storage area network". Nowhere in Twomey is a multiple protocol layer security system described or suggested. In fact, as stated by the Examiner: "The system includes a security processor for handling secure data traffic and utilizes security protocols (i.e. Ipsec)", Twomey shows only encryption/decryption based security at layer 3 (IP Layer) of the protocol hierarchy which is where Ipsec operates.

Accordingly, neither Williams nor Twomey explicitly teach, disclose, or illustrate each and every element of claim 2. Further, Applicant respectfully asserts that the combination of Williams and Twomey together fails to disclose or suggest all elements of claim 2. Hence, it would not have been obvious to one of ordinary skill in the art at the time the invention was made to have combined these two network security systems and arrive at all the features disclosed in claim 2. Further, if each element of claim 2 is considered by the Examiner to be inherent in the combination of Williams and Twomey, Applicant respectfully requests the introduction of extrinsic evidence clearly showing that the omitted material is necessarily present in the combination of Williams and Twomey and that it would be so recognized by persons of ordinary skill. In this regard, see In re Robertson, 49 USPQ2d 1949 (Fed. Cir. 1999). Alternatively, Applicant respectfully requests withdrawal of this rejection.

The arguments above as to claim 2 also apply to claims 20-25 which depend from claim 2.

New Claims 28-61

New claims 28-61 are submitted herewith. Neither Williams, Twomey, or any art of record or known to Applicant teach or suggest each and every element of each of the claims. Applicant respectfully submits that claims 28-61 are also allowable.

In view of these remarks, it is submitted that the claims of this application are patentably distinct from the references of record. Early notice of the claims is earnestly requested.

Applicant asserts that all claims are allowable and requests that the above rejections be withdrawn and the claims be passed to issue.

The Commissioner is hereby authorized to charge any additional fees or credit any overpayment that may be associated with this communication to Deposit Account No. 07-1896.

Respectfully submitted,
DLA PIPER RUDNICK GRAY CARY US LLP

Dated: November 22, 2004

By: _____
Peter R. Leal
Reg. No. 24,226
Attorney for Applicant

DLA PIPER RUDNICK GRAY CARY US LLP
2000 University Avenue
East Palo Alto, CA 94303-2248
Attn: Patent Department
Telephone: (916) 930-3239
Facsimile: (916) 930-3201

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Ashish Pandya
Serial No.: 10/783,890
Filed: February 20, 2004

Group Art Unit: 2667
Examiner: Not Yet Assigned
WRITTEN STATEMENT OF REASONS PRESENTED AT INTERVIEW

Attorney Docket No.: 2103110-991180
Customer No.: 26379
Title: Distributed Network Security System and a Hardware Processor Therefor

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as FIRST CLASS MAIL in an envelope addressed to: MAIL STOP AMENDMENT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on November 22, 2005.

Paula Borgens

Paula Borgens

* * *

WRITTEN STATEMENT OF REASONS PRESENTED AT INTERVIEW

MAIL STOP AMENDMENT
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant and his attorney wish to thank Supervisory Primary Examiner Pham for the courtesy of the telephone interview held at applicant's request on Tuesday, November 8.

Applicant discussed the rejections set forth in the Office Action mailed May 24, 2005. In accordance with 37 C.F.R. § 1.133(b), a complete written statement of the reasons presented at the interview as warranting favorable action with respect to that Office action is set forth below with respect to both of the rejections set forth therein.

First Rejection

Claims 1-27 were rejected as being anticipated by U.S. Patent Application No. 2003/0005331 ("Williams"). Applicant respectfully asserted that the rejection was respectfully traversed for the failure of Williams to include all elements and limitations of the rejected independent claims.

Regarding claim 1

1. The security devices of Williams operate only at layer 3 of the protocol hierarchy as stated in line 3 of 0073 of Williams; and

2. The multiple level security of Williams has 256 security levels which is totally different from OSI model with multiple protocol layer (for example, seven layers in the current protocol structure) which is required by claim 1 of applicant's invention.

Regarding claim 2

1. Williams does not teach, describe or suggest any elements of providing a security system for a storage area network, and the examiner acknowledges this at page 4, third paragraph of the Office action; and

2. The multiple level security of Williams has 256 security levels which is totally different from OSI model with multiple protocol layer (for example. seven layers in the current protocol structure) which is required by claim 2 in Applicant's invention.

Regarding claim 9

1. Nowhere in Williams is a plurality of networked systems comprising a hardware processor providing remote direct memory access capability described or suggested; and

2. Contrary to the requirement of claim 9, Williams clearly articulates at the second line of 0184 that direct access to the memory cannot be established; and

3. Williams fails to teach a security network system that operates by providing security at multiple protocol layers, despite the examiner's statements that Williams teaches a security network system that operates by providing security at two or more network layers of the OSI model with respect to Figure 4 and paragraphs 0073 and 0076 of Williams. Contrary to the examiner's statement, paragraph 0073 clearly states that security devices 18 operate within layer 3 of the protocol hierarchy.

Regarding claim 26

1. Williams fails to teach "a plurality of said set of systems comprising a hardware processor providing transport layer protocol processing"; and

2. Williams fails to teach that a security network system that operates by providing security at multiple protocol layers, despite the examiner's statements with respect to Figure 4 and the descriptions in paragraphs 0073 and 0076 of Williams.

Regarding claim 27

1. The first element requires "at least one of said networked systems having a hardware processor providing a protocol processing stack". Nowhere in Williams is a hardware processor providing a protocol processing stack described or suggested.

Second Rejection

Claims 2, 20-25 were rejected under 35 USC § 103(a) as being unpatentable over Williams in view of Twomey (U.S. Patent Application No. 2003/0131228).

Regarding claim 2

1. A combination of Williams and Twomey does not teach all of the described features of claim 2. Claim 2 requires both a combination for "providing a security system for a storage area network," and "a plurality of said set of systems comprising a hardware processor providing transport layer protocol processing."

2. Williams does not describe or suggest a plurality of networked systems comprising a hardware processor providing transport layer protocol processing.

3. Twomey also does not describe or suggest a transport layer protocol processing.

4. Thus, nowhere in Williams or Twomey is plurality of networked systems comprising a hardware processor providing transport layer protocol processing described or suggested.

5. As a second reason the combination of Williams and Twomey would not meet each element of claim 2 is that neither Williams nor Twomey teaches a security network system that operates by providing security at various network layers of the network layer hierarchy, despite the assertion by the examiner.

Dependent Claims

The above discussion was directed to only the independent claims. However, Applicant stated that all dependent claims are allowable as depending from independent claims that Applicant believes are allowable.

Result of Interview

No agreement was reached at the interview, although Supervisory Primary Examiner Pham indicated that he was inclined to withdraw Williams as a reference.

A detailed response to the Office action mailed May 24, 2005 is set forth in the Amendment filed on the same date as this paper.

The Commissioner is hereby authorized to charge any additional fees or credit any overpayment that may be associated with this communication to Deposit Account No. 07-1896.

Respectfully submitted,
DLA PIPER RUDNICK GRAY CARY US LLP

Dated: November 22, 2005

By: _____
Peter R. Leal
Reg. No. 24,226
Attorney for Applicant

DLA PIPER RUDNICK GRAY CARY US LLP
2000 University Avenue
East Palo Alto, CA 94303-2248
Attn: Patent Department
Telephone: (916) 930-3239
Facsimile: (916) 930-3201